REMARKS

Claims 1-21 were previously pending in this patent application. Claims 1-21 stand rejected. Herein, no Claim has been amended. Accordingly, after this Amendment and Response, Claims 1-21 remain pending in this patent application. Further examination and reconsideration in view of the claims, remarks, and arguments set forth below is respectfully requested.

35 U.S.C. Section 103(a) Rejections

Claims 1, 3, 4-10, 12-19, and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Janiak et al., U.S. Patent Application Publication No. 2002/0089410 (hereafter Janiak) in view of Maes et al., U.S. Patent No. 6,016,476 (hereafter Maes). These rejections are respectfully traversed.

Independent Claim 1 recites:

A method of enabling a user to access a computer system and activating said computer system, comprising the steps of:
a)   capturing biometric data from said user desiring access to said computer system having a user verification device in response to initial interaction by said user with said user verification device;
b)   verifying identity of said user using said biometric data; and
c)   ***if verification in said step b) is successful, powering-up said computer system to a normal operation mode and granting said user access to said computer system.*** (emphasis added)

It is respectfully asserted that there is no suggestion, motivation, or teaching found in the cited references (Janiak and Maes) to combine them.

Moreover, the combination of the cited references does not teach, suggest, or motivate all the limitations in Independent Claim 1.

Furthermore, Independent Claim 1 recites the limitation, "*if verification in said step b) is successful, powering-up said computer system to a normal operation mode and granting said user access to said computer system*" (emphasis added). In contrast, Janiak discloses a biometric solution comprising a host device (14) and a removable fingerprint identification module or FIM (12), wherein the FIM (12) works with the host device (14) such that the occurrence of a biometric match or non-match will allow the host device (14) to perform custom specific functionalities. [Janiak; Figure 1; paragraph [0179]]. While Janiak describes powering up the fingerprint sensor of the FIM (12) to obtain a fingerprint of a user, Janiak fails to disclose powering-up the host device (14) to a normal operation mode if verification of the user's identity by using the fingerprint (or biometric data) is successful, as in the invention of Independent Claim 1. In particular, Janiak simple describes using the biometric data to allow the host device (14) to perform custom specific functionalities and never describes the interaction between the powering on of the host device (14) and the FIM (12). Since the FIM (12) may be removed from the host device (14) when desired, this implies that the host device (14) is powered up without verification of the user's identity by using the user's fingerprint (or biometric data). [Janiak; Figure 1; paragraph [0021]].

Further, Maes is directed to utilizing biometric authorization to provide personal verification prior to processing user requested financial transactions and providing personal information. [Maes; Col. 1, lines 14-17]. In either the client/server mode or local mode, the PDA device (10) is fully powered, enabling the user to interact with the PDA device (10) before any biometric data is collected. [Maes; Col. 3, lines 38-67]. For the client/server mode, the user must periodically connect the powered PDA device (10) with a central server (60). [Maes; Col. 7, line 35 through Col. 8, line 27]. Once communication has been established, the user is prompted to enter certain verification data (e.g., biometric data). Id. For the local mode, the user selects a pre-enrolled credit card that is stored in memory (14) of the powered PDA device (10). [Maes; Col. 10, lines 29-65]. If the requested card information is found in memory (14), biometric verification must be performed before the card information can be written to the Universal Card (26). Id. In sum, the user is granted access to and interacts with the powered PDA device (10), wherein the user provides biometric data only when prompted by a specific transaction requested by the user. However, Maes does not disclose powering-up the computer system to a normal operation mode and granting the user access to the computer system if verification of captured biometric data from the user is successful, as in the invention of Independent Claim 1. Therefore, it is respectfully submitted that Independent Claim 1 is

patentable over the combination of Janiak and Maes and is in condition for allowance.

Dependent Claims 3-10 are dependent on allowable Independent Claim 1, which is allowable over the combination of Janiak and Maes. Hence, it is respectfully submitted that Dependent Claims 3-10 are patentable over the combination of Janiak and Maes for the reasons discussed above.

With respect to Independent Claim 12, it is respectfully submitted that Independent Claim 12 recites similar limitations as in Independent Claim 1. In particular, Independent Claim 12 is directed to a computer system. The computer system comprises a user verification device for capturing biometric data from a user, wherein the user initially interacts with the user verification device to gain access to the computer system. Further, the computer system includes a memory device, and a processor coupled to the user verification device and to the memory device, wherein the processor operative to receive the biometric data and to compare the biometric data with the reference template. If a match is determined, the computer system is powered-up from an inactive mode to a normal operation mode and the user is granted access to the computer system. Therefore, Independent Claim 12 is allowable over the

combination of Janiak and Maes for reasons discussed in connection with Independent Claim 1.

Dependent Claims 13-19 and 21 are dependent on allowable Independent Claim 12, which is allowable over the combination of Janiak and Maes. Hence, it is respectfully submitted that Dependent Claims 13-19 and 21 are patentable over the combination of Janiak and Maes for the reasons discussed above.

Claims 2, 11, and 20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Janiak et al., U.S. Patent Application Publication No. 2002/0089410 (hereafter Janiak), in view of Maes et al., U.S. Patent No. 6,016,476 (hereafter Maes), and further in view of Haitani et al., U.S. Patent No. 5,900,875 (hereafter Haitani). These rejections are respectfully traversed.

Dependent Claims 2 and 11 and Dependent Claims 20 are dependent on allowable Independent Claims 1 and 12 respectively, which are allowable over the combination of Janiak and Maes. Moreover, Haitani does not disclose capturing biometric data from the user desiring access to the computer system having a user verification device in response to initial interaction by the user with the user verification device. Further, Haitani does not disclose verifying identity of the user using the biometric data. Also, Haitani does not disclose if verification

of user's identity is successful, powering-up the computer system to a normal

operation mode and granting the user access to the computer system, as recited

in Claim 1 and similarly recited in Claim 12. Therefore Independent Claims 1 and

12 are patentable over the combination of Janiak, Maes, and Haitani. Since

Dependent Claims 2, 11, and 20 depend from Independent Claims 1 and 12, it is

respectfully submitted that Dependent Claims 2, 11, and 20 are patentable over

the combination of Janiak, Maes, and Haitani for the reasons discussed above.

CONCLUSION

It is respectfully submitted that the above claims, arguments, and remarks overcome all rejections. All remaining claims (Claims 1-21) are neither anticipated nor obvious in view of the cited references. For at least the above-presented reasons, it is respectfully submitted that all remaining claims (Claims 1-21) are now in condition for allowance.

The Examiner is urged to contact Applicant's undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Please charge any additional fees or apply any credits to our PTO deposit account number: 23-0085.

Respectfully submitted,

WAGNER, MURABITO & HAO, LLP

Dated: _8/2/2005_

Jose S. Garcia

Jose S. Garcia
Registration No. 43,628

Two North Market Street, Third Floor
San Jose, CA 95113
(408) 938-9060